

**Annual 47 C.F.R. § 64.2009(e) CPNI Certification**  
**EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for 2018 covering the prior calendar year 2017

Date filed: October 10, 2018

Name of company covered by this certification: **HRS Internet, LLC d/b/a LightBound**

Form 499 Filer ID: **825403**

Name of signatory: Jack Carr \_\_\_\_\_

Title of signatory: President & CEO

I, [Jack Carr], certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

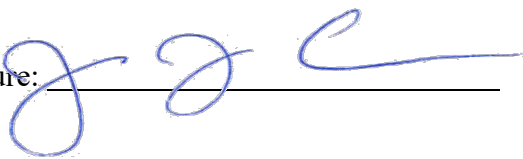
Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company **has not** taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company **has not** received any customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may be subject it to enforcement action.

Printed Name: Jack Carr Position: President & CEO

Signature:  Date: 10/10/2018

Attachment: Accompanying Statement explaining CPNI procedures

## STATEMENT EXPLAINING CPNI PROCEDURES

This statement explains how HRS Internet, LLC d/b/a LightBound's (the "Company") operating procedures ensure compliance with the FCC's CPNI rules.

1. The Company has a written CPNI policy manual that explains what CPNI is, when it may be used without customer approval, and when customer approval is required prior to CPNI being used, disclosed, or accessed for marketing purposes. The CPNI policy manual has been updated to account for all FCC CPNI rules and has been adopted the Company's board.
2. A CPNI Compliance officer has been designated to oversee all CPNI duties, training, and activity.
3. The Company has trained its employees about when they are, and are not, authorized to use or disclose CPNI.
  - A disciplinary process has been defined and is in place for violations and/or breaches of CPNI.
4. The Company ensures compliance with the FCC's authentication requirements.
  - All customers during a customer-initiated telephone call are authenticated as being an authorized account contact before discussing CPNI (non-call detail or call detail) without utilizing readily available biographical or account information as defined by the FCC.
  - Call detail is only released to customers during customer-initiated telephone contact if a password is provided. If the requesting customer does not provide a password, only the following FCC approved methods are permitted for the release of the requested call detail:
    - Sending the requested detail to the address of record (only a physical or email address associated with that particular account that has been in our company files for at least 30 days)
    - Calling the customer back at the telephone of record (only disclosing if the customer was authenticated as being an authorized account contact)
    - Having customer come in to Company's office and provide a valid government issued photo ID
5. The Company provides notification to customers of account changes. Customers are notified immediately when a customer creates or changes one of the following:
  - password
  - customer response to a back-up means of authentication for lost or forgotten passwords
  - online account
  - address of record
6. The Company implements the FCC's notice of unauthorized disclosure of CPNI

requirement by having a notification process in place in order to notify both law enforcement and customer(s) in the event of a CPNI breach within the timeline specified by the FCC.

7. The Company implements additional protection measures above and beyond the FCC CPNI rules.
  - The Company takes reasonable measures to discover and protect against activity that is indicative of pretexting
  - The Company maintains security of all CPNI, including but not limited to:
    - Shredding of documents containing CPNI
    - Locking of computer terminals when an employee is not at their station